



1. Gesetzesänderungen

+++ NEUE STANDARDDATENSCHUTZKLAUSELN BESCHLOSSEN +++

Die EU-Kommission hat am 4. Juni 2021 neue Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten in Drittländer beschlossen (Art. 46 Abs. 2 lit. c) DSGVO). Die neuen Klauseln sind modular aufgebaut und umfassen vier Konstellationen der Datenübermittlung:

- Verantwortlicher an Verantwortlichen (Modul 1)
- Verantwortlicher an Auftragsverarbeiter (Modul 2)
- Auftragsverarbeiter an (Unter-)Auftragsverarbeiter (Modul 3)
- Auftragsverarbeiter an Verantwortlichen (Modul 4)

Inhaltlich sollen die neuen Klauseln u. a. die Schrems-II Rechtsprechung des Europäischen Gerichtshofs (EuGH) berücksichtigen. Die Vertragsparteien müssen nun zwingend eine Risikoeinschätzung für die konkrete Datenübermittlung vornehmen und dokumentieren (auch „Transfer Impact Assessment“ genannt), die den Behörden auf Verlangen vorzulegen ist. Die neuen Standarddatenschutzklauseln lösen die bislang geltenden Standardvertragsklauseln ab. Unternehmen, die ihre Datenübermittlung auf die bisher geltenden Klauseln stützen, müssen diese binnen einer Übergangsfrist von

18 Monaten ersetzen.

[Zum Beschluss der EU-Kommission über die neuen Standarddatenschutzklauseln](#)
[Zur Pressemitteilung der EU-Kommission vom 4. Juni 2021 \(englisch\)](#)

+++ IT-SICHERHEITSGESETZ 2.0 TRITT IN KRAFT +++

Das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) wurde am 27. Mai 2021 verkündet. Das IT-Sicherheitsgesetz 2.0 erweitert die Kompetenzen und Aufgaben des Bundesamts für Sicherheit (BSI) und nimmt Änderungen an dem Gesetz über das BSI (BSiG) vor: Künftig unterfallen neben „Kritischen Infrastrukturen“ und „digitalen Diensten“ auch „Unternehmen im besonderen öffentlichen Interesse“ den Pflichten des BSiG. Hierzu gehören etwa Unternehmen und Zulieferer mit volkswirtschaftlich besonders großer Bedeutung für Deutschland. Das IT-Sicherheitsgesetz 2.0 trat überwiegend bereits am 28. Mai 2021 in Kraft, einzelne Regelungen treten jedoch erst am 1. Dezember 2021 in Kraft.

[Zum IT-Sicherheitsgesetz 2.0](#)

[Kurz-Übersicht des BSI zum IT-Sicherheitsgesetz 2.0](#)

+++ BETRIEBSRÄTEMODERNISIERUNGSGESETZ: ARBEITGEBER FÜR DATENVERARBEITUNG DES BETRIEBSRATS VERANTWORTLICH +++

Das Gesetz zur Förderung der Betriebsratswahlen und der Betriebsratsarbeit in einer digitalen Arbeitswelt (Betriebsrätemodernisierungsgesetz) ist am 18. Juni 2021 in Kraft getreten. Das Gesetz sieht u. a. vor, dass der Arbeitgeber datenschutzrechtlich verantwortlich ist für die Verarbeitung von Beschäftigtendaten durch den Betriebsrat. Dies gilt aber nur, wenn der Betriebsrat die Daten zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben verarbeitet. Damit ist der Datenschutzbeauftragte des Arbeitgebers auch für die Datenverarbeitungen des Betriebsrats zuständig. Die vorstehenden Fragen waren vor dieser gesetzlichen Klarstellung heftig umstritten.

[Zum Betriebsrätemodernisierungsgesetz](#)

2. Rechtsprechung

+++ EUGH: BELGISCHE DATENSCHUTZBEHÖRDE FÜR DSGVO-VERSTÖßE VON FACEBOOK IRELAND ZUSTÄNDIG +++

Der EuGH hat entschieden, dass nationale Datenschutzbehörden in Ausnahmefällen vor einem Gericht im Inland gegen DSGVO-Verstöße eines Unternehmens vorgehen können, obwohl dessen Hauptniederlassung – und damit die eigentlich zuständige sog. federführende Behörde – in einem anderen Mitgliedstaat liegt. In dem Fall hatte die belgische Datenschutzbehörde vor einem inländischen Gericht gegen die Facebook Ireland mit Sitz in Irland wegen Verstößen bei der Verarbeitung von Daten belgischer

Nutzer geklagt. Facebook hatte argumentiert, die Behörde agiere außerhalb ihrer Zuständigkeit, da die für grenzüberschreitende Verarbeitungen zuständige federführende Behörde in Irland liege. Der EuGH stellte nun klar, dass die belgische Behörde im Rahmen des Kohärenzverfahrens (Art. 60 ff. DSGVO) gegen Facebook Irland vorgehen kann und insoweit auch Klage vor belgischen Gerichten einreichen darf, selbst wenn Facebook keine eigene Niederlassung in Belgien unterhält.

[Zur Pressemitteilung des EuGH \(v. 15. Juni 2021 – C-645/19\)](#)

+++ AG WIESBADEN: SAMMLUNG MEHRERER VERTRÄGE IN ORDNER FÜHRT ZU ANWENDBARKEIT DER DSGVO +++

Das Amtsgericht Wiesbaden (AG Wiesbaden) hat festgestellt, dass dem Mieter einer Wohnung ein Auskunftsanspruch nach Art. 15 DSGVO gegen die Vermieterin zusteht, die mehrere Wohnungen als Privatperson vermietete. Die Vermieterin hatte ihre Mietverträge nicht digital gespeichert, sondern nur physisch in einem Ordner abgeheftet. Diese Sammlung stellte nach Ansicht des Gerichts ein Dateisystem im Sinne der DSGVO dar, sodass die Vorschriften der DSGVO anwendbar seien. Die Vermieterin hatte zudem Namen und Telefonnummer des Mieters in einem Mobiltelefon gespeichert. Hierin erkannte das Gericht eine automatisierte Datenverarbeitung, sodass die DSGVO auch aus diesem Grund anwendbar sei.

[Zum Urteil des AG Wiesbaden \(v. 26. April 2021, Az. 93 C 2338/20\)](#)

+++ LG KÖLN ZUR FORMULIERUNG VON COOKIE-BANNERN +++

Das Landgericht Köln (LG Köln) hat entschieden, dass die nachfolgende Formulierung in einem Cookie-Banner rechtswidrig ist:

„Um unsere Website für Sie optimal zu gestalten und fortlaufend verbessern zu können, verwenden wir Cookies. Durch die weitere Nutzung der Webseite stimmen Sie der Verwendung von Cookies zu.“

Die Vorschrift verstoße gegen § 15 Abs. 3 Telemediengesetz (TMG). Der Bundesgerichtshof legt diese Vorschrift dahingehend aus, dass Nutzer ihre ausdrückliche Einwilligung in die Erstellung von Nutzerprofilen für Werbezwecke erteilen müssen (siehe hierzu den [BB-Sondernewsletter Mai 2020](#)).

[Zum Beschluss des LG Köln \(v. 13. April 2021 – 31 O 36/21\)](#)

+++ CONSEIL D'ÉTAT WEIST KLAGE WEGEN DROHENDER DATENÜBERMITTLUNG IN USA AB +++

Das oberste französische Verwaltungsgericht (Conseil d'État) hat eine Klage wegen der Nutzung des Hosting-Anbieters Amazon Web Services Sarl (AWS), einer

Tochtergesellschaft der amerikanischen Amazon Web Services Inc., abgewiesen. Ein Auftragsverarbeiter des französischen Gesundheitsministeriums nutzte die Dienste von AWS in Zusammenhang mit einer Plattform zur Verwaltung von Impfterminen. Die Kläger befürchteten, dass personenbezogene Daten von dieser Plattform in die USA übermittelt werden könnten. Der Conseil d'État stellte klar, dass für diesen Fall hinreichende zusätzliche Maßnahmen getroffen worden seien, die ein angemessenes Schutzniveau in den USA herstellten. Die getroffenen Maßnahmen sahen u. a. eine Verschlüsselung der Daten vor der Übermittlung an AWS vor, wobei der Schlüssel bei einer Dritten Partei mit Sitz in Frankreich treuhänderisch verwahrt wurde, sodass AWS selbst keinen Zugriff auf Klardaten hatte. Der Conseil d'État wies ausdrücklich darauf hin, dass an AWS keine Gesundheitsdaten, die als besonders sensibel gelten, übermittelt worden seien. Hintergrund der Entscheidung ist die sog. Schrems-II Entscheidung des EuGH (Urt. v. 16.7.2020, C311/18, siehe [BB Datenschutz-Ticker Juli 2020](#)).

[Zur Entscheidung des Conseil d'État \(v. 12. März 2021, n° 450163\)](#)

3. Behördliche Maßnahmen

+++ DEUTSCHE DATENSCHUTZBEHÖRDEN KONTROLLIEREN UMSETZUNG DES SCHREMS II-URTEILS +++

Diverse deutsche Datenschutzbehörden haben angekündigt, im Rahmen einer abgestimmten länderübergreifenden Kontrolle die Datenübermittlungen durch Unternehmen in Drittstaaten zu überprüfen, um die Umsetzung der Anforderungen des Schrems II-Urteils des EuGH sicherzustellen. Zu diesem Zweck werden Unternehmen aktuell umfangreiche Fragebögen zugesendet, die folgende Themenbereiche betreffen: den Einsatz von Dienstleistern zum E-Mail-Versand, zum Hosting von Internetseiten, zum Webtracking, zur Verwaltung von Bewerberdaten sowie den konzerninternen Austausch von Kundendaten und Daten der Beschäftigten. Nach aktuellem Kenntnisstand beteiligen sich die Landesdatenschutzbehörden von Bayern, Berlin, Brandenburg, Hamburg, Niedersachsen, Rheinland-Pfalz und dem Saarland an diesen Kontrollen.

[Zur Pressemitteilung des Hamburgischen Datenschutzbeauftragten, inkl. Fragebögen](#)

+++ NIEDERLÄNDISCHE DATENSCHUTZBEHÖRDE VERHÄNGT BUßGELD ÜBER EUR 525.000 WEGEN FEHLENDEM UNIONSVERTRETER +++

Die Datenschutzbehörde der Niederlande Autoriteit Persoonsgegevens (AP) hat gegen den nicht-europäischen Betreiber einer Webseite ein Bußgeld in Höhe von

EUR 525.000 verhängt. Der Betreiber hatte keinen Unionsvertreter benannt, obwohl er dies nach Ansicht der Behörde gemäß Art. 27 DSGVO hätte tun müssen. Die Vorschrift verpflichtet Verantwortliche und Auftragsverarbeiter, die ausschließlich in einem Drittstaat niedergelassen sind, einen Vertreter innerhalb der Union als Verpflichtungs- und Vollstreckungssubjekt zu benennen.

[Zur Entscheidung der AP \(niederländisch\)](#)

+++ LUXEMBURGISCHE DATENSCHUTZBEHÖRDE: REKORDBUßGELD GEGEN AMAZON ERWARTET +++

Die luxemburgische Datenschutzbehörde Nationale Kommission für den Datenschutz (CNPD) plant laut einem Zeitungsbericht des Wall Street Journal die Verhängung eines Bußgelds in Höhe von ca. EUR 350 Mio. gegen Amazon. Die CNPD ist als federführende Behörde für Datenverarbeitungen des Amazon Konzerns in Europa zuständig. Sie habe den weiteren betroffenen Datenschutzbehörden im Rahmen des Kohärenzverfahrens (Art. 60 ff. DSGVO) einen Entwurf des Bescheids übersendet. Es ist derzeit nicht bekannt, welche Datenschutzverstöße Amazon im Einzelnen vorgeworfen werden.

[Zur deutschen frei verfügbaren Meldung auf Heise Online](#)

4. Stellungnahmen

+++ EU-BEHÖRDEN VERÖFFENTLICHEN AKTUALISIERTE EMPFEHLUNGEN ZUM DRITTLANDTRANSFER +++

Der Europäische Datenschutzausschuss (EDSA) hat eine aktualisierte Fassung der Empfehlungen über zusätzliche Maßnahmen zur Absicherung von Datentransfers in Drittländer veröffentlicht. Eine erste Version dieser Empfehlungen stammt bereits aus November 2020 (siehe [BB Datenschutz-Ticker November 2020](#)). Der EDSA hält auch in der aktualisierten Fassung an der empfohlenen 6-Stufen Prüfung für Datentransfers in Drittländer fest (*1. Know your transfer; 2. Verify transfer tool; 3. Assess legal system in the third country; 4. Consider supplementary measures; 5. Take formal procedural steps; 6. Re-evaluate*). Zudem erklärt der EDSA zusätzliche Schutzmaßnahmen, die Unternehmen neben dem Abschluss von EU-Standarddatenschutzklauseln ergreifen sollen, um ein angemessenes Datenschutzniveau im Drittstaat zu gewährleisten.

[Zu den Empfehlungen des EDSA vom 18. Juni 2021 \(englisch\)](#)

[Zu den Empfehlungen des EDSA für die Bewertung staatlicher Zugriffsbefugnisse im Drittland vom 10. November 2020 \(englisch\)](#)

Ihre Ansprechpartner

Redaktion (verantwortlich)

Dr. Andreas Lober

Zur Newsletter Anmeldung
E-Mail weiterleiten



Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie künftig keine Informationen erhalten möchten, können Sie sich jederzeit abmelden.

© BEITEN BURKHARDT

Rechtsanwaltsgesellschaft mbH

Alle Rechte vorbehalten 2021

Impressum

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH

(Herausgeber)

Ganghoferstraße 33, 80339 München

AG München HR B 155350/USt.-Idnr: DE-811218811

Weitere Informationen (Impressumsangaben) unter:

<https://www.beiten-burkhardt.com/de/impressum>